FY2012 Information Security Awareness

Oct. 1, 2011

USDA

Table of Contents

FY 2012 Information Security Awareness Training

Welcome to FY 2012 Information Security Awareness and Rules of Behavior Training!

This training is mandatory for all USDA employees, contractors, partners, and volunteers. New employees, contractors, partners, and volunteers are required to complete the awareness training prior to gaining access to systems. All users must stay abreast of security policies, requirements, and issues. Users must make a conscientious effort to avert security breaches by staying alert to network vulnerabilities.

By taking this course, you are meeting the legal requirement for all users of federal information systems to take annual computer security awareness training. This course is designed to help you understand the importance of information systems security, or ISS, its guiding principles, and what it means for your agency. This course also provides the "Rules of Behavior" that govern your use of USDA information technology (IT) resources.

It will identify potential risks and vulnerabilities associated with federal information systems, review your role in protecting these systems, and provide guidelines to follow at work to protect against attacks on information systems.

Key Topics

Social Engineering

Kate got a phone call from a man who says he is investigating an information system security breach and needs her to verify her password. He sounds very authoritative, and Kate doesn't want to get into trouble.

Do you know what steps to take if this happens to you?

Phishing

Linda just got an email from her bank saying her debit card may have been stolen. In order to protect herself from fraud and any charges to her account, the email

instructs her to send an email reply immediately in order to confirm her account and PIN numbers.

What would you do in this situation?

Mobile Code

At lunch, Mike's friend raved about a hilarious new website and emailed him the link. But a computer message says the site needs to install and run an ActiveX application in order for Mike to view it.

Would you click Install or Cancel?

Hoaxes

Phyllis receives an email from a friend warning that a dangerous and fast-moving new computer virus is wreaking havoc on computer networks around the world. Phyllis observes that her friend sent the warning to her entire email distribution list to try to protect her contacts.

What action would you take?

Password Security

John feels like he always has to change his password on his work computer. He tends to forget which password he is using for what. He's gotten into a habit of jotting them down on a sticky note and keeping them tucked away under his keyboard.

How safe and secure is your password?

Course Overview

This course consists of four (4) lessons.

- Lesson 1: Importance of Information Systems Security
- Lesson 2: Threats to Information Systems Security
- Lesson 3: Malicious Code
- Lesson 4: User Roles and Responsibilities

Lesson 1: Importance of Information Systems Security

The Importance of Information Systems Security lesson will introduce the principles of ISS, their evolution, and ISS-related policies, laws, and Rules of Behavior. It will also introduce the critical infrastructure protection program.

Learning Objective

After completing this lesson, you should be able to:

- Identify what information systems security is and why it is important.

Lesson 2: Threats to Information Systems Security

The Threats to Information Systems Security lesson will explain the difference between threats and vulnerabilities. It will also provide information regarding various types of threats.

Learning Objective

After completing this lesson, you should be able to:

- Differentiate between a threat and vulnerability, and identify the risks associated with each.

Lesson 3: Malicious Code

The Malicious Code lesson will introduce the concept of malicious code, including the impact and methods used to infect information systems.

Learning Objective

After completing this lesson, you should be able to:

- Identify the threat posed by malicious code and identify how to protect federal information systems from malicious code.

Lesson 4: User Roles and Responsibilities

The User Roles and Responsibilities lesson will identify important guidelines for ensuring a secure system, define classification levels for federal information, and outline your role as a user in protecting this information.

Learning Objectives

After completing this lesson, you should be able to:

- Recognize the classification levels for federal information and identify what you must do to help protect federal information.
- Identify your responsibilities and the "Rules of Behavior" that govern the use of USDA IT resources.

Lesson 1: Importance of Information Systems Security (ISS) and Rules of Behavior

The Internet has made it extremely easy to quickly obtain and transfer information. While global connectivity is very convenient, it also increases our vulnerability to

outside attacks. The goals of ISS and the Rules of Behavior are to protect our information and information systems.

ISS and Rules of Behavior protect information from unauthorized access or modification and ensure that information systems are available to their users. This means that a secure information system maintains confidentiality, integrity, and availability.

Learning Objective
After completing this lesson, you should be able to:

- Identify what information systems security is and why it is important.

This lesson includes the following topics:

- History of ISS
- ISS and Rules of Behavior Legal Requirements
- Rules of Behavior – Acceptable Behavior and Penalites
- Critical Infrastructure

History of ISS

Fifty years ago, computer systems presented relatively simple security challenges. They were expensive, understood by only a few, and isolated in controlled facilities.

Protecting these computer systems consisted of controlling access to the computer room and clearing the small number of specialists who needed such access.

As computer systems evolved, connectivity expanded, first by remote terminals, and eventually by local and wide-area networks, or LANs and WANs.

As the size and price of computers came down, microprocessors began to appear in the workplace and homes all across the world.

What was once a collection of separate systems is now best understood as a single, globally connected network. ISS now includes infrastructures neither owned, nor controlled by the federal government. Because of this global connectivity, a risk to one is a risk to all.

ISS and Rules of Behavior Legal Requirements

It is important that you are aware of the possibility of attacks against federal systems and the method in which potential attacks could occur.

Understanding your responsibilities for protecting information resources and how you can contribute to preventing attacks will contribute to the safety of federal information systems.

USDA is required by law to ensure that anyone who utilizes USDA IT resources is aware of his or her responsibilities and complies with the established Rules of Behavior.

What you should know
The Federal Information Security Management Act, or FISMA (part of the E-Government Act of 2002, Public Law 107-347 dated December 17, 2002), and the Office of Management and Budget (OMB) Circular A-130 require that all users of federal computer systems be trained in information systems security concerns and comply with the established Rules of Behavior. U.S. Office of Personnel Management (OPM) regulations also require each agency to have computer security awareness training.

Knowledge Check #1

Fill in the blank.
All of the following are important aspects of Information Systems Security, except _____.

1. Protecting information on government computer networks
2. Blocking unauthorized access to government computer networks
3. Preventing digital modification to government computer networks
4. Specific written restrictions for the use of government computer networks

The correct answer can be found on page 11.

Rules of Behavior – Acceptable Behavior and Penalties

Rules of Behavior establish expected and acceptable computing behaviors. Because written guidance cannot cover every contingency, users are also required to use sound judgment and the highest ethical standards in their decision making.
USDA will take corrective action and/or enforce the use of penalties against any user who violates any USDA or Federal system security policy, using any and/or all of the following:

- Corrective actions (taken in accordance with existing rules, regulations, and laws) include written reprimands, temporary suspension from duty, reassignment or demotion, and termination of Federal employment.
- Suspension of system privileges.
- Possible criminal prosecution.

What you should know
The following nonofficial activities are prohibited on any government owned or leased computer:

- Gambling.
- Intentionally visiting and downloading material from pornographic websites.
- Lobbying Congress or any government agency.
- Campaigning – political activity.
- Any type of continuous audio or video streaming from commercial, private, news, or financial organizations, except as expressly authorized by management.
- Activities that are connected with any type of outside employment.
- Endorsement of any non-government products, services, or organizations.

Critical Infrastructure

Critical Infrastructure Protection, or CIP, is a national program established to protect our nation's critical infrastructures. Critical infrastructure refers to the physical and cyber-based systems essential to the minimum operations of the economy and government.

Sectors considered part of our nation's critical infrastructure include, but are not limited to, information technology and telecommunications, energy, banking and finance, transportation and border security, water, and emergency services. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. However, these infrastructures have become increasingly automated and interlinked. Increased connectivity creates new vulnerabilities.

Critical Infrastructure – Threats

Equipment failures, human error, weather, as well as physical and cyber attacks impacting one sector, could potentially impact our nation's entire critical infrastructure. For example, if the natural gas supply is disrupted by a computer virus, and electrical power is cut, computers and communications would shut down. Roads, air traffic, and rail transportation would be impacted. Emergency services would be hampered. An entire region can be debilitated because an element critical to our infrastructure has been attacked.

CIP was established to define and implement proactive measures to protect our critical infrastructure and respond to any attacks that occur.

Knowledge Check #2

Select the correct answer.
Which of the following systems would not be included in the national Critical Infrastructure Protection program?

1. Social Security
2. Electric Power
3. Elementary Schools
4. The Federal Reserve

The correct answer can be found on page 17.

The correct answer to Knowledge Check #1 is: Specific written restrictions for the use of government computer networks. Written guidance cannot cover every possible scenario for the use of a government computer.

Lesson 2: Threats to Information Systems Security

It is important to understand the difference between threats and vulnerabilities and how they can affect your system.

A threat is any circumstance or event that can potentially harm an information system by destroying it, disclosing the information stored on the system, adversely modifying data, or making the system unavailable.

A vulnerability is a weakness in an information system or its components that could be exploited. Vulnerabilities exist when there is a flaw or weakness in hardware or software that could be exploited by hackers. Vulnerabilities are frequently the result of a flaw in the coding of software. To correct a vulnerability, a vendor would issue a fix in the form of a patch to the software.

Learning Objective

After completing this lesson, you should be able to:

- Differentiate between a threat and vulnerability, and identify the risks associated with each.

This lesson includes the following topics:

- Threat Categories
- Environmental Threats
- Internal vs. External Human Threats

- Social Engineering
- Rules of Behavior – Access
- Incident Reporting
- Phishing
- Cookies
- Mobile Code
- Peer-to-Peer (P2P)
- Rules of Behavior - Software

Threat Categories

There are two types of threat categories: environmental and human threats.

Environmental Threats

Natural environmental events - including lightning, fires, hurricanes, tornadoes, or floods - pose threats to your system and information. A system's environment - including poor building wiring or insufficient cooling for the systems - can also cause harm to information systems.

How can you protect against environmental threats?
Rules of Behavior – Hardware/Environmental Threats

Users should do their best to protect computer equipment from damage, abuse, theft, and unauthorized use. Users shall protect computer equipment from hazards such as:

- Extreme temperatures;
- Electrical storms;
- Water and fire;
- Static electricity;
- Spills from food and drink;
- Dropped objects;
- Excessive dusty environments; and
- Combustible materials.

Internal vs. External Human Threats

Human threats can be internal or external. An internal threat can be a malicious or disgruntled user, a user in the employ of terrorist groups or foreign countries, or self-inflicted unintentional damage, such as an accident or bad habit.

An external threat can be hackers, terrorist groups, foreign countries, or protesters.

Let's look more closely at human threats to federal information systems. The greatest threats to federal information systems are internal - from people who have working knowledge of and access to their organization's computer resources.

An internal threat, or insider, is any person with legitimate physical or administrative access to the computer who can misuse or exploit weaknesses in the system. Others, due to a lack of training and awareness, can also cause damage. Although there are security programs to prevent unauthorized access to information systems, and employees undergo background investigations, certain life experiences can alter people's normal behavior and cause them to act illegally. Stress, divorce, financial problems, or frustrations with co-workers or the organization are some examples of what might turn a trusted user into an insider threat.

How can you protect against internal human threats?

Rules of Behavior – Internal Threats

Users shall:

- Keep an inventory of all equipment assigned to them.
- Only use equipment for which they have been granted authorization.
- Not leave computer equipment in a parked car or in an unsecured location where it might be stolen.
- Follow established procedures when removing equipment from USDA premises. This usually requires a property pass.
- Not install or use unauthorized software or hardware on the network, including personal laptop computers, pocket computers, or personal digital assistants and network enabled cellular phones, except as expressly authorized.
- Not alter the configuration, including installing software or peripherals, on government equipment unless authorized.

- Notify management before relocating computing resources.
- When possible, use physical locking devices for laptop computers and exercise additional care for other portable devices.

External Threats

External threats, or outsiders, are most commonly hackers. An outsider is an individual who does not have authorized access to an organization's computer system.

What you should know.
Today, hackers may include representatives of foreign countries, terrorist groups, or organized crime. Today's hacker is also far more advanced in computer skills and has access to hacking software that provides the capability to quickly and easily identify a system's security weaknesses. Using tools available on the Internet, a hacker is capable of running automated attack applications against thousands of host computers at a time. Because of this, hackers pose a serious risk to the security of federal information systems.

Social Engineering

When Kate answered the phone, the man on the other end sounded very authoritative. He said he was investigating a possible security incident on USDA's Web TA time and attendance information system and needed her to verify her password. Kate may have been the target of social engineering.

Social engineering is a hacking technique that relies on human nature. This approach is used by many hackers to obtain information valuable to accessing a secure system.

Rather than using software to identify security weaknesses, hackers attempt to trick an individual into revealing passwords and other information that can compromise your system security.

They use people's inherent nature to trust to learn passwords, logon IDs, server names, operating systems, or other sensitive information.

For example, a hacker may attempt to gain system information from an employee by posing as a service technician or system administrator with an urgent access problem.

Nobody should ever ask you for your passwords. This includes system administrators and help desk personnel.

Your Role in Social Engineering

Understanding social engineering behaviors will enable you to recognize them and avoid providing important security information to unauthorized sources.

Preventing social engineering:

- Verify identity.
- Do not give out passwords.
- Do not give out employee information.
- Do not follow commands from unverified sources.
- Do not distribute dial-in phone numbers to any computer system except to valid users.
- Do not participate in telephone surveys.

Reacting to social engineering:

- Use Caller ID to document phone number.
- Take detailed notes.
- Get person's name/position.
- Report incidents.

Rules of Behavior – Social Engineering

Users are responsible and accountable for any actions taken under their user ID.

What you should know.

Users shall:

- Protect passwords from access by other individuals.
- Never give a password to another person, including a supervisor or a computer support person.
- Not ask anyone for their password.
- Construct effective passwords by following USDA password policy for complex passwords.

Rules of Behavior – Access

Users shall access and use only information for which they have official authorization.

What you should know.
Users shall:

- Follow established procedures for accessing information, including use of user identification, user authentication, passwords, and other physical and logical safeguards.
- Follow established channels for requesting and disseminating information.
- Access only those files, directories, and applications for which access authorization by the system administrator has been granted.
- Use government equipment only for approved purposes.

In addition, users shall NOT:

- Give information to other employees or outside individuals who do not have access authority.
- Store sensitive or confidential information on a system unless access control safeguards (e.g., passwords, locked rooms, and protected local area network (LAN) storage areas) are used.
- Use their trusted position and access rights to exploit system controls or access data for any reason other than in the performance of official duties.
- Browse other users' files (i.e., what can be accessed).

Knowledge Check #3

Select the correct answer.
Kate got a phone call from a man who says he is investigating a possible security incident on USDA's Web TA time and attendance information system and needs her to verify her password. What can Kate do to prevent or discourage this from being a case of a hacker using social engineering?

1. Verify the caller's identity by getting his name and position.
2. Not give out her password.
3. Take detailed notes and report the call to her supervisor.
4. All of the above. All of the answers are methods for preventing computer hackers from using social engineering.

The correct answer can be found on page 19.

The correct answer to Knowledge Check #2 is: Elementary Schools. Critical infrastructure refers to the physical and cyber-based systems essential to the minimum operations of the economy and government.

Incident Reporting

Each user is responsible for reporting any form of security violation, whether waste, fraud, or abuse through the USDA incident reporting mechanism.

What you need to know.
Users shall:

- Report security incidents, or any incidents of suspected fraud, waste, or misuse of USDA resources or release of USDA personally identifiable information (PII) to the USDA Help Desk (1-888-926-2373) or PII Hotline (1-877-PII-2-YOU), or to the appropriate agency IT Information Security Manager.
- Report security vulnerabilities and violations as quickly as possible to the USDA Help Desk (1-888-926-2373) or USDA PII Hotline (1-877-PII-2-YOU), or to the appropriate agency IT Information Security Manager so that corrective action can be taken.
- Take reasonable action immediately upon discovering a violation to prevent additional damage, such as logging out of a terminal or locking up property.
- Cooperate willingly with official action plans for dealing with security violations.

Phishing

Linda received an email from her bank that her debit card account may be at risk and she needs to verify her account and PIN numbers. Is someone "phishing" for Linda's private information?

A social engineering scam that you need to be aware of is phishing. Phishing is a high-tech scam that uses email or websites to deceive users into disclosing credit card numbers, bank account information, social security number, passwords, or other sensitive information.

Phishers send an email or pop-up message that claims to be from a business or organization that a user deals with. For example, phishers often pose as a user's Internet online payment service, or even a government agency. The message usually says that the user needs to update or validate account information and may threaten some dire consequence if the user does not respond. The message directs the user to

a website that looks just like a legitimate site but it is not affiliated with the organization in any way. The purpose of the bogus site is to trick the user into divulging personal information so the operators can steal the user's identity and run up bills or commit crimes in the user's name. The bogus site may also install malicious code on the user's system.

If you receive an email or pop-up message that asks for personal or financial information, do not reply or click on the link in the message.

Legitimate companies do not ask for this information via email. If you are concerned about your account, contact the organization identified in the email using a telephone number you know to be genuine.

A recent real life example of social engineering occurred when a U.S. government employee, visiting another country, provided his business card to several people. A few months later, a highly-visible U.S. government official received an "official-looking" email containing an attachment from a valid ".gov" address. Fortunately, the recipient did not open the email attachment, but instead, sent the email back to the person whom he thought sent it to him for verification.

It turns out that the originating email spoofed the email address of the government employee who traveled to the foreign country. The attachment contained malicious code.

Cookies

There are several security risks associated with browsing the Internet. One common risk is known as cookies.

A cookie is a text file that a web server stores on your hard drive when you visit a website. The web server retrieves the cookie whenever you revisit that website. When you return, the cookie recognizes you, saving you the trouble of re-registering.

The most serious security problem with cookies has occurred when the cookie has 'saved' unencrypted personal information, such as credit card numbers or Social Security numbers, in order to facilitate future business with that site. Another problem with cookies is that the site can potentially track your activities on the web.

To reduce the risk associated with cookies, and better protect your system, your browser should be set up not to accept cookies.

Mobile Code

Mike wants to see a funny website his friend told him about, but first he has to load and run an application to see the website. If Mike runs the application, he may be vulnerable to malicious Mobile Code.

Mobile code, such as ActiveX and Java, are scripting languages used for Internet applications.

Mobile code embedded in a web page can recognize and respond to user events such as mouse clicks, form input, and page navigation. It can also play audio clips.

However, it does introduce some security risks. Mobile code can automatically run hostile programs on your computer without your knowledge simply because you visited a web site. The downloaded program could try to access or damage the data on your machine or insert a virus.

Review your agency's policies for specific guidance or restrictions on the use of mobile code.

Knowledge Check #4

Fill in the blank.
Linda received an email from her bank asking her to verify her account and PIN numbers to prevent identity theft. This could be a form of information security risk known as _____.

1. a hoax
2. Phishing
3. Email engineering
4. Stealing cookies

The correct answer can be found on page 22.

The correct answer for Knowledge Check #3 is: All of the above. All of the answers are methods for preventing computer hackers from using social engineering.

Peer-to-Peer (P2P)

Peer-to-peer, or P2P, refers to file sharing applications, such as Morpheus and BitTorrent, that enable computers connected to the Internet to transfer files to each other.

P2P Vulnerabilities

Peer-to-peer software enables files to be accessed and transferred with ease.

Music files, pornography, and movie files are the most commonly transferred files using unauthorized peer-to-peer software. Obtaining these files at no cost raises not only ethical concerns, but could result in criminal or civil liability for illegal duplication and sharing of copyrighted material. In addition, participating in peer-to-peer file sharing increases your vulnerability. Opening up your computer via the Internet provides outsiders a link into your system, creates risk, and enables the possibility for a breach in security.

The following list provides examples of some P2P software divided by category.
Instant Messaging/Telephony:

- Yahoo! Messenger
- Windows Live Messenger
- Skype
- AOL Instant Messenger

File Sharing:

- BitTorrent
- Gnutella
- Kazaa
- WinMX
- Napster
- PC Anywhere
- eDonkey
- Morpheus
- eMule
- LimeWire
- BearShare
- Timbuktu

Rules of Behavior – P2P File Sharing

Peer-to-peer connections are a common avenue for the spread of computer viruses and spyware.

The installation and use of unauthorized peer-to-peer applications can also result in significant vulnerabilities to your agency's networks, including exposure to unauthorized access of information and compromise of network configurations.

The Office of Management and Budget (OMB) requires all Agencies to develop guidance on the use of peer-to-peer applications.

Contact your security point of contact for further information on your specific policy regarding the use of peer-to-peer applications.

What you need to know.
Users are prohibited from using peer-to-peer (P2P) file sharing. P2P file sharing poses a threat to IT security. It allows employees to transfer files between computers without proper security controls. These programs can be used to distribute inappropriate materials, violate copyright law and put government information at risk. Users should be familiar with the USDA P2P file sharing policy located on the USDA directives intranet site.

Rules of Behavior – Software

Users shall not install non-authorized, standard, public domain, or shareware software on their computer without approval from the appropriate management official. Computer users must protect USDA owned software and equipment from malicious software.

What you need to know.
Users shall NOT:

- Use USDA purchased software on personally owned or non-USDA computers unless authorized.
- Alter the configuration, including installing software or peripherals, on government computer equipment unless authorized.
- Download, install, or run security programs or utilities that might reveal weaknesses in the security measures or access privileges of any system unless otherwise expressly authorized.

In addition, users shall:

- Comply with all software licensing agreements and Federal copyright laws.

Knowledge Check #5

Fill in the blank.

Mike wants to check out the link to a funny website his friend told him about, but needs to install and run an ActiveX application first. ActiveX is a form of Mobile Code. All of the following are functions of Mobile Code, except _____.

1. Plays audio clips.
2. Inserts a computer virus.
3. Enables encrypted cell phone communication.
4. Controls webpage navigation.

The correct answer can be found on page 24.

The correct answer for Knowledge Check #4 is: Phishing. Phishing is a high-tech scam that uses email or websites to deceive users into disclosing credit card numbers, bank account information, social security number, passwords, or other sensitive information.

Lesson 3: Malicious Code

Malicious code is defined as software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

It is designed with the intent to deny, destroy, modify, or impede system configurations, programs, or data files.

Malicious code comes in several forms including viruses, Trojan horses, and worms.

The most common methods for the spread of malicious code are through email attachments and downloading files from the Internet, but you can also receive malicious code just by visiting an infected web site.

Learning Objective

After completing this lesson, you should be able to:

- Identify the threat posed by malicious code and identify how to protect federal information systems from malicious code.

This lesson includes the following topics:

- Email and Attachments
- Hoaxes

Email and Attachments

Email messages and email attachments provide a common route to transfer malicious code.

Always be cautious when opening email attachments – they may contain malicious code that could corrupt files, erase your hard drive, or enable a hacker to gain access to your computer.

Some examples of file types that users should be suspicious of include: .exe, .com, .vbs, .bat, .rar, .cmd, .js, .pif, and .shs.

Don't assume that an attachment is safe because a friend or coworker sent it. Some malicious code is activated by merely opening the message. Save the attachment to your hard drive and scan it with up-to-date anti-virus software before opening it.

What you need to know.

Protect Your Computer System

- Scan email attachments and outside files using current anti-virus software.
- Ensure system is scanned daily.
- Delete email from unknown or unexpected sources.
- Turn off email software option to automatically download attachments.

Respond to Virus Attack

- Do not email a copy of the infected file.
- Contact your agency help desk or security contact.

Hoaxes

An email Phyllis gets from a good friend includes a warning about a serious computer virus. Her friend says to tell everyone she knows. If Phyllis forwards the email to her office email group, is she helping or promoting an “Internet Hoax?”

Internet hoaxes are email messages designed to influence you to forward them to everyone you know.

Hoaxes encourage you to forward email messages by warning of new viruses, promoting moneymaking schemes, or citing a fictitious cause. By encouraging mass distribution, hoaxes clog networks and slow down Internet and email service for computer users.

If you receive an email message requesting that you forward it to all your friends and coworkers, do not forward the email.

Knowledge Check #6

Select the correct answer.
Phyllis receives an email with an attached file about a computer virus from a friend she trusts. What step should Phyllis take before opening the attachment on her computer?

1. Since the email is from someone she trusts, it is OK to go ahead an open it.
2. Forward the email to her personal email account and open the attachment from there.
3. Forward the email to a coworker and ask them to open it.
4. Save the attachment to her computer hard drive and scan it with her computer's anti-virus software.

The correct answer can be found on page 27.

The correct answer for Knowledge Check #5 is: Enables encrypted cell phone communication. Mobile code embedded in a web page can recognize and respond to user events such as mouse clicks, controls page navigation, plays audio clips, and can run hostile programs on your computer.

Lesson 4: User Roles and Responsibilities

As an authorized user of federal information systems, you have certain responsibilities and need to remember your right to privacy is limited when using a government computer.

Any activity conducted on a government system can be monitored. Each time you log on to a government system, you consent to being monitored. You should use your computer for government business only.

Avoid government computer misuse. Examples of computer misuse are: viewing or downloading pornography, gambling on the Internet, conducting private commercial business activities or profit-making ventures, loading personal software, or making unauthorized configuration changes.

Learning Objectives

After completing this lesson, you should be able to:

- Recognize the classification levels for federal information and identify what you must do to help protect federal information.

- Identify your responsibilities and the "Rules of Behavior" that govern the use of USDA IT resources.

This lesson includes the following topics:

- Basic User Guidelines
- Rules of Behavior – Accountability
- Rules of Behavior – Appropriate Email Use
- Tips for Creating a Secure Password
- Classified and Unclassified Information
- Media Devices
- Wireless Networks
- Personal Identifiable Information

Basic User Guidelines

There are eight basic generally accepted ethical guidelines that should govern your actions when using a government computer system.

Ethical guidelines

- Do not use computer for harm.
- Do not interfere with others work.
- Do not snoop in other's files.
- Do not use a computer to commit crimes.
- Do not use or copy unlicensed software.
- Do not steal intellectual property.
- Do not use a computer to pose as someone else.
- Do not use computer resources without approval.

Rules of Behavior – Accountability

In addition to adhering to ethical guidelines, all users are accountable for actions related to information resources entrusted to them.

Users shall:

- Behave in an ethically, informed, and trustworthy manner when using systems.
- Be alert to threats and vulnerabilities such as malicious programs and viruses.
- Participate in IT security training and awareness programs.
- Not install or use unauthorized software on USDA equipment.
- Comply with all software licensing agreements and not violate Federal copyright laws.
- Know that your system may be monitored and that there is no expectation of privacy on USDA IT resources.

In addition, users shall prevent others from using their accounts by:

- Logging out or locking the screen when leaving the vicinity of their terminals or PCs.
- Setting a password on automatic screen savers.
- Helping to remedy security breaches, regardless of who is at fault.
- Immediately notifying the system administrator whenever there is a change in role, assignment, or employment status and/or when access to the system is no longer required.
- Complying with a system's rules of behavior when accessing external systems.
- Reading and understanding banner pages and end user licensing agreements.

Rules of Behavior – Integrity

Users must protect the integrity and quality of information. This includes, but is not limited to:

- Reviewing quality of information as it is collected, generated, and used to ensure that it is accurate, complete, and up-to-date.
- Taking appropriate training before using a system to learn how to correctly enter and change data.
- Protecting information against viruses and similar malicious code by:

  - Using up-to-date anti-virus software.
  - Avoiding use of unapproved software, such as shareware and public domain software.
  - Discontinuing use of a system at the first sign of virus infection.
- Never knowingly entering unauthorized, inaccurate, or false information into a system.

Knowledge Check #7

Select the correct answer.

Peggy is the office computer guru and often solves her coworkers' computer issues before IT can help. Peggy frequently finds that she can get her own work done faster by downloading free shareware tools than with the software provided with her office computer. Which of the following policies is Peggy violating?

1. Basic Ethical Guidelines
2. Accountability Rules of Behavior
3. Integrity Rules of Behavior
4. All of the above

The correct answer can be found on page 30.

The correct answer for Knowledge Check #6 is: Save the attachment to her computer hard drive and scan it with her computer's anti-virus software. Do NOT assume that an attachment is safe because it was sent by a friend or coworker.

Rules of Behavior – Email: Appropriate Email Use

The following rules apply regarding email activity:

- Automatic filters will be in place to help prevent inappropriate and offensive messages from passing through USDA email gateways.
- Any email on a government email system is the property of the government and may become an official record.
- The use of IT resources constitutes consent to possible monitoring and security testing. Monitoring and security testing ensures proper security procedures and appropriate usage are being observed for USDA IT resources.
- Monitoring of email and other IT resources by management will be done only in accordance with established USDA policy and guidelines.

- Users are prohibited from using USDA IT resources to send, receive, retain, or proliferate any messages or material that is fraudulent, inappropriate, offensive, harassing, or is of a sexual nature.

Email is also for official business. Your organization may permit some incidental and casual email use.

Guidelines on the types of personal email use that may or may not be authorized are as follows:

- Email use may not adversely affect the performance of official duties.
- Email use must not reflect poorly on the government.
- You may not use government email to send pornographic, racist, sexist, or otherwise offensive emails, send chain letters, or sell anything.
- Email use must not overburden the system, as happens when you send mass emails.
- To keep networks open and running efficiently, don't forward jokes, pictures, or inspirational stories.
- Similarly, avoid using "Reply All" unless it is absolutely necessary.
- Personal email use may be authorized if it is of reasonable duration and frequency, preferably on employees' personal time, such as on a lunch break.

Email is also permissible when it serves a legitimate public interest, such as allowing employees to search for a job in response to federal government downsizing.

Public Key Infrastructure

Federal information systems identify and authenticate each user either through a smart card login or user ID and password.

The preferred method of access to information systems is through the use of public key infrastructure, or PKI, which enables your agency to issue electronic keys, called digital certificates, to authorized users.

PKI allows users to encrypt and digitally sign emails and documents.

Tips for Creating a Secure Password

John thinks having to change passwords frequently and memorize them is complicated and inconvenient. So he writes them down and leaves them under his

computer keyboard. Maybe John just needs some tips for creating secure passwords that he can remember?

Many federal information systems still identify and authenticate users by his or her user ID and password. The user ID and password determines the user's right to access the system.

Remember, it is your responsibility to ensure that all activity performed under your user ID is appropriate use of federal information systems resources.

What you need to know.
It is important to create a complex password in order to protect government information systems from being compromised.

- Combine letters, numbers, special characters. (ex: !,@,#,$)
- Use alphanumeric combinations or phrase associations. (ex: P@$$w0rd T1p$)
- Avoid words or phrases that can be found in the dictionary.
- Avoid using personal information. (ex: birthday, home address, phone number)
- Memorize password and refrain from writing it down.
- Change passwords regularly.

Physical Security

Protecting federal information systems and the information they contain starts with physical security.

Physical security includes protection of the entire facility, from the outside perimeter to the offices inside the building, including all the information systems and infrastructure.

You are responsible for knowing your organization's physical security policies and following them. Your organization should have procedures for gaining entry, procedures for securing your work area at night, and emergency procedures.

These may include:

- The use of a badge or key code for entry;
- Locking your cubicle;

- Undocking your laptop and storing it in a separate location;
- Locking data storage devices, such as hard drives and USB drives, before you leave for the evening and during emergency procedures such as fire alarms.

Physical Security – Proactive Approach

You should also make sure others follow your organization's physical security policies and challenge people who don't. Don't allow people to gain entrance to a building or office by following someone else instead of using their own badge or key code.

Challenge people who do not display badges or passes. If you are the last person to leave in the evening, make sure that others have secured their equipment properly.

Finally, you are responsible for reporting any suspicious activity that you see.

Knowledge Check #8

Fill in the blank.
John is trying to do a better job with password security. All of the following are guidelines for creating a secure password, except _____.

1. John replaces some of the letters in his passwords with special characters like @ and $.
2. John uses the name the street he lives on as his password so he can remember it easily.
3. John uses alphanumeric combinations and phrase associations, like $m311y C@t, to make his passwords more complex.
4. Now that he's gotten into the habit, John changes his passwords every couple of weeks.

The correct answer can be found on page 34.

The correct answer for Knowledge Check #7 is: All of the above. Installing any unapproved software on a government computer violates basic user ethical guidelines, and rules of behavior for both accountability and integrity.

Inventory Control

Part of physical security includes controlling the inventory of equipment that stores federal information. When government laptops are lost or stolen, so is the information that is on them. In recent years, federal inventory control procedures have been tightened in response to the loss of thousands of government laptop computers.

Federal agencies are responsible for controlling their inventory of office and computer equipment, including phones, computers, printers, faxes, monitors, and USB drives.

When you receive government property, you should sign for it. Once it has been signed out to you, you are then responsible for that equipment and taking the necessary precautions to ensure that it doesn't get lost or stolen.

To remove equipment from the building, or bring equipment into the building, your organization may require you to have a property pass signed by the property manager.

If that property is lost or stolen, follow your organization's procedures for reporting the loss. In addition to reporting the loss of the equipment itself, you must report the loss of the information that was on the equipment, and the significance of that lost information.

Telework Procedures

Telework, also known as telecommuting, is emerging as a viable option for many government employees. Advances in computer and telecommunications capabilities make telework increasingly practical.

There are risks associated with remote access to your government computer network.

If you have received approval for teleworking, you are required to satisfy the requirements in your agency's policies and guidelines.

Classified and Unclassified Information

All federal information, combined with the right conditions and circumstances, could provide an adversary insight into our capabilities and intentions. In addition, the aggregation of unclassified information can elevate the sensitivity level of information.

Thus, even unclassified information, if compromised, could impact the safety of our personnel and systems.

All federal unclassified information not specifically cleared for public release requires some level of security protection. At a minimum, it must be reviewed before it is released, in any form, outside the U.S. government. Each agency has its own unclassified information policy. Contact your security point of contact for additional information on your agency's policy.

What you need to know.

Unclassified Information

- Unclassified information includes “For Official Use Only" or FOUO; “Controlled Unclassified Information” or CUI; and “Sensitive But Unclassified” or SBU.
- Examples are personnel, financial, payroll, medical, operational, and Privacy Act information.
- CUI must be stored in a locked drawer or secure container. When it is no longer needed, it should be destroyed.

Classified Information

- Classified information includes “Confidential,” “Secret,” or “Top Secret.”
- The specific level of classification is determined by the original classification authority.
- Classified information must be used in an area that has been approved and cleared for the appropriate classification level.
- When not in use, classified information must be stored in a General Services Administration (GSA) approved vault or container.

Backups, Storage, and Labeling

A large amount of federal information is stored on removable media such as CDs, USB drives, or removable hard drives and you need to take extra precaution to protect them from loss or theft.

Important files MUST be backed up regularly and stored in a secure locationto minimize the loss of data if your hard drive crashes or is infected by a virus.

Store all removable mediain solid storage containers, such as metal cabinets, to protect against fire and water damage.

It is very important to label all removable media, including backups, and the contents of the media, to reflect the classification or sensitivity level of the information the media contains.

Removable media must be properly marked and stored according to the security classification of information it contains.

When you no longer need the information, you should not erase, or "sanitize" it. Removable media must be degaussed or destroyed if it is not reused at the same or higher classification level of the system in which it was used.

Follow your agency's policies regarding handling, storage, labeling, and destruction of removable media.

Rules of Behavior – Backups, Storage, and Labeling

Computer systems and media must be protected from environmental hazards such as fire, water, heat, and food spills. They must also be protected from theft, unauthorized alteration, and careless handling.

What you need to know.
Users shall:

- Use physical and logical protective measures such as the following to prevent loss of availability of information and systems.
    - Ensure that there are backups of information for which they are responsible.
    - Protect systems and media where information is stored.
    - Store media in protective jackets.
- Keep media away from devices that produce magnetic fields (such as phones, radios, and magnets).
- Follow contingency plans.

Knowledge Check #9

Select the correct answer.
David wants to use some newly published administrative guidelines for his agency as an example for a paper he is writing for a business class. There are no markings on the guidelines indicating their security classification. David should:

1. Assume the guidelines are not classified and go ahead and use them for his assignment.
2. Review the guidelines for any personal information about other USDA employees, and use a black marker to hide that information before using the guidelines for his assignment.
3. Contact his agency's security point of contact to seek permission to use the guidelines for his assignment.

4. Remove all references to his agency from the guidelines document before using it for his assignment.

The correct answer can be found on page 37.

The correct answer for Knowledge Check #8 is: John uses the name the street he lives on as his password so he can remember it easily. John should avoid using personal information for his passwords. Instead, he should be using recognizable phase associations.

Media Devices

Be extremely careful when using cell phones, smart phones, laptop and tablet computers, fax machines, and wireless networks. You need to be as vigilant about security on these devices as you are with your computer at work.

Cell Phones and Smart Phones

If you use a cell phone or smart phone, anyone with the right equipment could potentially listen to your conversation. Cell phones are merely transmitters.

Use a landline for more privacy, and never discuss sensitive information on an unsecured phone.

Smart phones, pose an additional security threat for a number of reasons.

Their small size and relatively low cost make them easy to obtain and difficult to control.

They have tremendous connectivity and storage capabilities, and are extremely popular. It can be very easy for a person to set up a smart phone to download information from your computer.

All smart phones connecting to government systems should be in compliance with your agency's policy and OMB guidance.

Laptops, Tablets and Fax Machines

The convenience of laptop and tablet personal computers (PC), and other portable computing devices makes them extremely vulnerable to theft or security breaches.

User logon information should always be password protected.

Be careful what you display on your screen when it is visible to others, especially in close quarters, such as on airplanes.

Maintain possession of your PC at all times when traveling. When you reach your destination, be sure that your PC is properly secured when left unattended.

If your PC has wireless capability, ensure that security features are properly configured IAW your agency's wireless policy. When not in use, laptop wireless should be turned "off" or, if this is not possible, configured to connect to recognized Internet access points, not ad hoc networks.

An Office of Management and Budget (OMB) memorandum states: All sensitive data stored on laptops and other portable computer devices should be encrypted. Ensure that you follow both your agency's and OMB's guidance on encryption of sensitive data on laptops.

When transmitting sensitive information over a fax machine, ensure that the recipient will be present to pick up the fax immediately. Contact the recipient directly to confirm receipt of the fax. Never transmit classified information via an unsecured fax machine.

Always use a cover sheet so that the content of your fax isn't immediately visible.

Wireless Networks

Wireless networks operate by using radio signals, instead of traditional computer cables, to transmit and receive data.

Unauthorized users with a receiver can intercept your communications and access your network.

This is dangerous because unauthorized users may be able to capture not only the data you are transmitting, but also any data stored on your network.

Rules of Behavior – Wireless Networks

All USDA employees and contractors are prohibited from using any unauthorized 802.11x network devices within USDA buildings. Users must ensure that any wireless capable devices in their control, including laptops, PDAs, and Bluetooth telephones, have their wireless networking disabled. The only acceptable use of wireless communications is through the USDA provided messaging service.

Wireless is vulnerable because unauthorized users may be able to capture not only the data you are transmitting, but also any data stored on your network.

Ensure you are in compliance with your agency's policy regarding the use of wireless technologies.

Spillage

Spillage, also referred to as contamination, is when information of a higher classification level is introduced to a network at a lower classification level. It is the improper storage, transmission, or processing of classified information on an unclassified system.

An example would be when information classified as Secret is introduced to an unclassified network. Any user who identifies or suspects that a spillage has occurred should immediately notify his or her security point of contact.

Cleaning up after a spillage is a resource intensive process. It can take roughly three weeks to contain and clean an affected information system. Be aware that spillages can greatly impact the security of federal information.

Helpful hints:

- Check all emails for possible classified information.
- Mark and store all removable media properly.
- Ensure all file names and subject headers reveal the sensitivity of the information.

Personal Identifiable Information (PII)

The Privacy Act, signed into law in 1975, requires the government to safeguard information about individuals that is processed by Federal agencies or contractor computer systems. The Act also requires the government to provide access to the information by the individual and to amend the information if it is not accurate, timely, complete, or relevant.

What you should know.

New guidance concerning greater measures for protection of Personally Identifiable Information (PII) is outlined in several OMB memoranda.

For example, OMB requires that lost or stolen PII be reported within one hour to the U.S. Computer Emergency Response Team, or CERT.

Each agency has its own policies to implement OMB's guidance. Check with your security point of contact for additional PII requirements.

As an authorized user, you should ensure that PII is protected on Federal computer systems.

Your Responsibility

Information is a critical asset to the U.S. government. It is your responsibility to protect government sensitive and classified information that has been entrusted to you.

Please contact your security point of contact for more information about classification or handling of information.

Knowledge Check #10

Fill in the blank.
USDA Employee Kyle is working at his desk when he realizes his wallet containing his government identification card is missing. OMB guidance for protection of Personally Identifiable Information requires Kyle to report the missing wallet to the Computer Emergency Response Team _____.

1. as soon as possible
2. within one hour
3. by the close of the business day
4. within 24 hours

The correct answer can be found on page 37.

The correct answer for Knowledge Check #9 is: Contact his agency's security point of contact to seek permission to use the guidelines for his assignment. Since David can't tell if the information has been cleared for public release, he should contact his agency's security point of contact and seek permission to use the guidelines.

The correct answer to Knowledge Check #10: within one hour. OMB requires that lost or stolen PII be reported to CERT within one hour.

Acknowledgment of USDA Rules of Behavior and Next Steps

Congratulations!

You have almost completed the "FY2012 USDA Information Security Awareness and Rules of Behavior" training course. However, you must still complete an assessment with a score of 70% or higher to receive credit for this training. Please contact your supervisor or Human Resources representative for instructions on obtaining a copy of this assessment.

USDA is required by law to ensure that anyone who utilizes USDA Information Technology (IT) resources is aware of his or her responsibilities and complies with these Rules of Behavior.

This confirms that I successfully completed the training. I have read and understand the Rules of Behavior as identified in the Departmental Manual on Personnel Security (see http://www.ocio.usda.gov/directives/doc/DM3545-000.pdf for details).

Signature: _____

Date: _____

Per Departmental Regulation 3620-001, AgLearn is the official training system for USDA, and the source of all data for audits, mandatory training completions, and records examinations relating to personnel actions. All data contained in AgLearn is subject to examination by the USDA Inspector General and/or the Office of Personnel Management without notice at any time. False claims of completed training submitted by employees using AgLearn as recorded in their Learning History file, if substantiated, may be used to support disciplinary or other administrative actions.